REMARKS

The headings and the specification have been replaced by new headings which are not underlined or in bold type, and are all in uppercase letters.

Initially, the claims have been amended such that independent claims 1 and 19 have been limited to the subject matter of encrypting using a crossed-inverse quasigroup.

Claim 29 has been similarly amended, and also specifies the decryption of the message using the same crossed-inverse quasigroup.

Claim 34 has been canceled.

Claims 1, 4, 11, 22 and 34 stand rejected based on Seheidt. Claim 1 has been amended to include the limitations of claim 2 therein; thus, obviating this rejection with regards to claim 1. Claim 19 has been amended to include the limitations of claim 20 thereby obviating this rejection.

Claims 2, 3, 5, 6, 8, 9, 14-16 and 19-21 stand rejected over 35 USC 103 based on Seheidt in view of Scheidt. This contention is respectfully traversed. Claim 1 as amended has the scope of original claim 2, which recites encrypting using a crossed-inverse quasigroup. The rejection states that Scheidt shows encrypting using a nontrivial crossed-inverse quasigroup to encode, drawing attention to column 2, lines 46-53. However,

this is respectfully traversed: Scheidt teaches nothing about a crossed-inverse quasigroup. The cited section of Scheidt describes an encryption technique where the decryption key is the inverse of the encryption key. However, note that mathematically, decryption must inherently be the inverse of encryption, in order to get the same results that you put in. This is not a group or quasigroup, but rather teaches only an encryption key where the decryption key has certain characteristics of the inverse of the encryption.

A group is a special collection of objects as described in the specification on page 6 such that all operations between any two items in the group is again within the group; see, page 6, lines 15-21. A quasigroup is a special item which does not obey the associative rule that (a . b) . c = a . (b . c), where the . represents an operation, for all a, b and c. There is no teaching or suggestion of using crossed inverse quasigroups in Scheidt. Rather, Scheidt teaches using a modulo-W system (see, generally, columns 7 and 8). There is nc teaching or suggestion that this represents a crossed-inverse quasigroup, as claimed.

Moreover, even though Scheidt teaches using a decryption key which is the inverse of the encryption key, it never teaches or suggests any use of a crossed-inverse quasigroup.

Encryption relies on use of big numbers, and large amounts of computation. A specific advantage noted by the inventors is that the use of a crossed-inverse quasigroup avoids having to compute a complete inverse table in order to decrypt a communication. If a crossed-inverse quasigroup is used, then the same table can be used both to encrypt the communication and to decrypt the communication. There is no teaching or suggestion of this subject matter in Seheidt or in Seheidt in view of Scheidt. Quite simply, while Scheidt does teach a mathematical formula with modulus, it teaches nothing about a crossed-inverse quasigroup.

Therefore, claim 1, which now defines the use of a nontrivial crossed-inverse quasigroup should be allowable, along with claims 3-16 and which depend therefrom. Nothing in the hypothetical combination of prior art teaches or suggests the use of a crossed-inverse quasigroup.

Claim 19 has been amended to recite a crossed-inverse quasigroup, and hence claim 19 should be allowable along with claims 21-26 which depend therefrom.

Claim 29 has been amended to recite encrypting the message using a crossed-inverse quasigroup, sending the message, and decrypting the message using the same crossed-inverse quasigroup. Hence, this is in no way taught or suggested in any

of the cited prior art, and this claim should be allowable along with claims 31-33 which depend therefrom.

It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

In view of the above amendments and remarks, therefore, all of the claim should be in condition for allowance. A formal notice to that effect is respectfully solicited.

Attorney Docket No. 06666-032001
Serial No. 09/576,598
Amendment dated June 30, 2004
Reply to Office Action dated March 30, 2004

Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: June 30, 2004

Scott C. Harris
Reg. No. 32,030

Fish & Richardson P.C.
PTO Customer Number: 20985
12390 El Camino Real
San Diego, CA 92130
Telephone: (858) 678-5070
Facsimile: (858) 678-5099
10410755.doc